



U.S. Department of Justice

United States Attorney
Southern District of New York

86 Chambers Street
New York, New York 10007

June 19, 2025

By ECF

The Honorable Denise L. Cote
United States District Judge
United States Courthouse
500 Pearl St.
New York, NY 10007

Re: *Am. Fed'n of Gov't Emps., AFL-CIO, et al. v. U.S. Office of Personnel Mgmt., et al.*, No. 25 Civ. 1237 (DLC)

Dear Judge Cote:

This Office represents Defendants in the above-referenced case. Pursuant to the Court's direction at the teleconference held on June 13, 2025, we write respectfully to provide the Court with Defendants' revised proposal concerning the terms of the Court's draft preliminary injunction order in this matter.¹ Defendants make this submission without waiving and explicitly reserving any and all defenses, arguments and rights to appeal. Defendants also write to provide the Court with an overview of the most salient issues Defendants identified after review of the Court's draft preliminary injunction order, and during the parties' meet and confer regarding the same.² Defendants appreciate the opportunity to further address these issues with the Court at tomorrow's teleconference.

Defendants' Revised Proposal

While Defendants continue to maintain that preliminary injunctive relief is unwarranted in this matter, they have submitted a revised proposal to address the stated goals outlined by the Court at the June 13th conference. The first paragraph of Defendants' revised proposal seeks to provide the Court with the set of representations that Your Honor requested concerning OPM's commitment to adherence to the requirements of the Privacy Act with respect to any new grant of administrative access permission going forward, and the processes and procedures that OPM has put in place in response to this litigation and similar litigation in the District of Maryland to address concerns related to compliance with the Privacy Act. *See* Tr. 3:7-23.³

¹ Defendants' revised proposed preliminary injunction order is attached to this submission.

² Defendants acknowledge that the Court requested that the parties submit letters limited to two to three pages explaining their proposed preliminary injunction orders but respectfully are providing a lengthier submission in order to appropriately address all of these issues.

³ "Tr." citations are to the transcript of the teleconference held by the Court on June 13, 2025.

The second paragraph of Defendants’ revised proposal outlines a report concerning OPM’s grant of administrative access permissions to “DOGE Agents,”⁴ where such administrative access permissions are currently effective—*i.e.*, where such individuals currently have administrative access. This report essentially requires OPM to conduct a periodic review of access permissions, in keeping with the principles of least privilege and separation of duties, *see* ECF No. 121 at 27-28, and provides the information the Court has requested regarding OPM “DOGE Agents.”

This paragraph also addresses the distinct “final agency action” the Court found to be at issue. In its Opinion and Order, the Court defined the “final agency action” in this case as “[t]he decision to give access to DOGE agents.” ECF No. 121 at 88. Specifically, Plaintiffs have consistently alleged, *see, e.g.*, Compl. ¶ 9; ECF No. 84 at 2, ECF No. 109 at 1, and this Court has found that the type of access at issue in this case is “administrative access”—not regular user access. ECF No. 121 at 88 (“OPM leadership demanded administrative access to multiple OPM systems for DOGE agents.”); *see also id.* at 81 (“It is especially unlikely that any DOGE agents ever needed administrative access to any OPM systems.”). This paragraph also addresses the “increased [] risk of cybersecurity breaches,” *id.* at 95, which the Court determined was occasioned by granting DOGE agents administrative access. *See also id.* (“[T]he wide-ranging access that OPM granted to the DOGE agents would be considered a security risk in the private sector.”). Finally, this proposal acknowledges the reality that there can be no continued increase to the agency’s “attack surface,” *id.* at 66, where such users no longer have such administrative access permissions. As a result, Defendants’ revised proposal is narrowly tailored to address the specific violations of the Privacy Act the Court found, while not imposing unnecessary burdens on OPM’s day-to-day operations. *See Waldman Pub. Corp. v. Landoll, Inc.*, 43 F.3d 775, 785 (2d Cir. 1994) (a preliminary injunction “should be narrowly tailored to fit specific legal violations,” and “should not impose unnecessary burdens on lawful activity.” (citation omitted)).

Defendants’ revised proposal thus provides most, if not all, of the assurances the Court has requested, while not “interfer[ing] in any way with the efficient operation” of OPM. Tr. 4:16-17; 7:18-22. This remedy essentially represents “remand without vacatur”—a remedy that is entirely appropriate where vacatur (revoking access permissions) would have “disruptive consequences.” *See NRDC v. EPA*, No. 19 Civ. 5174 (DLC), 2020 WL 2769491, at *1 (S.D.N.Y. Apr. 15, 2020) (quotation and citation omitted). In contrast, Plaintiffs’ revised proposal would revoke DOGE Agents’ access immediately, unduly “restrict[ing] disclosure [where] the agency in good faith believes disclosure should be given.” Tr. 7:20-22.

The Court Does Not Have Authority to Enter a Preliminary Injunction Order Requiring OPM to Conduct Forensic Audits

This Court does not have authority to order OPM to undertake the three proposed forensic audits pursuant to a preliminary injunction order under the Administrative Procedure Act (“APA”). Like Federal Rule of Civil Procedure 65, Section 705 of the APA empowers courts to enter preliminary injunctive relief “to maintain the status quo.” *See Comprehensive Cmty. Dev. Corp. v.*

⁴ The second paragraph of Defendants’ proposal also incorporates a revised definition of “DOGE Agents” that is clearly stated and administrable by OPM. *See* Fed. R. Civ. P. 65(d)(1)(B)-(C).

Sebelius, No. 12 Civ. 0776 (PAE), 2012 WL 738185, at *8 (S.D.N.Y. Mar. 7, 2012). However, the APA does not permit a court to exercise continuing oversight over agency operations to ensure compliance with the broad statutory mandates of the Privacy Act, and it does not permit a court to order an agency to conduct a series of forensic audits that the agency is not required by law to undertake. *See Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 65 (2004) (“*SUWA*”) (“The limitation to *required* agency action rules out judicial direction of even discrete agency action that is not demanded by law.” (emphasis in original)).

The Court’s first and second proposed audits concerning access to OPM’s data systems—mandated every month and every week, respectively—amount to continuing, and impermissible, judicial oversight of OPM’s administrative operations with respect to its obligations under the Privacy Act. The Court may not impose these recurring audits to determine whether OPM has complied with the broad statutory mandates of the Privacy Act. *See id.* at 66-67 (“If courts were empowered to enter general orders compelling compliance with broad statutory mandates, they would necessarily be empowered, as well, to determine whether compliance was achieved—which would mean that it would ultimately become the task of the supervising court, rather than the agency, to work out compliance with the broad statutory mandate, injecting the judge into day-to-day agency management.”). Such week-to-week (or month-to-month) judicial oversight is “foreclosed by the APA, and rightly so.” *City of New York v. U.S. Dep’t of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) (under the APA, courts do not “adjudicate generalized grievances asking us to improve an agency’s performance or operations,” and cannot “engage in day-to-day oversight of the executive’s administrative practices”).

At bottom, Plaintiffs and this Court “cannot seek wholesale improvement of [OPM’s Privacy Act compliance] by court decree, rather than in the offices of the [agency] or the halls of Congress, where programmatic improvements are normally made.” *Lujan v. Nat’l Wildlife Fed’n*, 497 U.S. 871, 891 (1990). The Court’s three proposed forensic audits would be in addition to separate audits already being conducted by the Government Accountability Office⁵ and by OPM’s independent Office of the Inspector General (“OIG”)⁶ concerning “DOGE access” to OPM’s data

⁵ *A Review of the Fiscal Year 2026 Budget Requests for the Congressional Budget Office, the Government Accountability Office, and the Government Publishing Office: Hearing Before the Subcomm. on the Legislative Branch of the S. Comm. on Appropriations*, 119th Cong. (Apr. 29, 2025) (Testimony of Gene L. Dodaro, Comptroller General, Government Accountability Office) (“Right now we are auditing the DOGE access, as to what access they had, what changes, we’re looking at the digital footprint within each of these major systems across government, we’re at Social Security, Treasury, OPM, and others. So, we’ll have a better idea about what impact DOGE’s access has had on the data systems, and whether there’s been any information input into the system or taken out of the system.”), available at <https://www.appropriations.senate.gov/hearings/a-review-of-the-fiscal-year-2026-budget-requests-for-the-congressional-budget-office-the-government-accountability-office-and-the-government-publishing-office> (timestamp: 41:30).

⁶ Letter from OPM Acting Inspector General Norbert E. Vint to Rep. Gerald E. Connolly (Mar. 7, 2025) (noting that OPM OIG has incorporated Rep. Connolly’s February 6 request to conduct a

systems. Indeed, OPM OIG already conducts an annual evaluation and audit of OPM’s information technology security program and practices—including data protection and privacy—to ensure compliance with the Federal Information Security Management Act. *See, e.g.,* OPM OIG, *Final Audit Report: Federal Information Security Modernization Act Audit – Fiscal Year 2023* (Oct. 30, 2024), *available at*

<https://www.oversight.gov/sites/default/files/documents/reports/2024-11/2024-ISAG-008.pdf>.

Having identified deficiencies with OPM’s compliance with the Privacy Act, the Court cannot now direct the agency how best to achieve compliance. *See Allina Health Servs. v. Sebelius*, 746 F.3d 1102, 1111 (D.C. Cir. 2014) (“[T]he court erred by directing the Secretary how to calculate the hospitals’ reimbursements, rather than just remanding after identifying the error.” (citing *SEC v. Chenery Corp.*, 332 U.S. 194, 201 (1947))). The Court similarly cannot impose on OPM such requirements “to make sure that OPM has done a reliable, complete audit of access by DOGE agents,” Tr. 10:1-3, to “identify any copies of records or copies of information from records,” that may have been made at the direction of DOGE agents, ECF No. 129-1 at 5, or require that OPM “assess any risks to its cybersecurity that have resulted or may result,” from its granting of administrative access, *id.* at 5-6. The APA “sets forth the full extent of judicial authority to review executive agency action for procedural correctness.” *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 513 (2009). While the APA does permit a reviewing court to “hold unlawful and set aside agency action . . . found to be arbitrary, capricious . . . or otherwise not in accordance with law,” § 706(2)(A), in such cases, “the proper remedy under § 706(2) would be to remand to the agency for further administrative proceedings.” *Comprehensive Cmty. Dev. Corp.*, 2012 WL 738185, at *8 (citing *Nat. v. Ass’n of Home Builders v. Defenders of Wildlife*, 551 U.S. 644, 658 (2007)).⁷ Stated differently, this Court cannot impose its preferred methodology on OPM to fulfill its duties under the Privacy Act. *See Cobell v. Norton*, 392 F.3d 461, 476 (D.C. Cir. 2004) (vacating district court’s order where it “seem[ed] a specification not of [the agency’s] duties but of the court’s preferred methodology for assuring [the agency’s] fulfillment of those duties”).

review of “DOGE Team” access to data systems at OPM), *available at* <https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/hogr-minority-final.pdf>.

⁷ While courts are empowered to “compel agency action unlawfully withheld or unreasonably delayed,” 5 U.S.C. § 706(1), that section applies only where “an agency failed to take a *discrete* agency action that it is *required to take*,” *SUWA*, 542 U.S. at 64 (emphasis in original). That provision of the APA is not at issue in this litigation. And “where an agency is *not required* to do something, [a court] cannot compel the agency to act—let alone to act faster.” *Gonzalez v. Cuccinelli*, 985 F.3d 357, 366 (4th Cir. 2021) (emphasis in original). The only statutory mandate concerning an accounting of disclosures under the Privacy Act is found at 5 U.S.C. § 552a(c), and specifically exempts disclosures made pursuant to § 552a(b)(1)—the provision at issue in this litigation.

The Court's Proposed Audits Do Not Have a Basis in the Court's Findings of Fact or Conclusions of Law

The three forensic audits proposed by the Court (and now Plaintiffs) have no basis in the Court's findings of fact or conclusions of law and are otherwise unsupported by the evidentiary record. Even in a case outside of the APA context, a district court can only order preliminary injunctive relief that is “narrowly tailored to fit specific legal violations,” and must be based on factual findings in the evidentiary record. *See Waldman Pub. Corp.*, 43 F.3d at 785; *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 120 (2d Cir. 2009) (finding district court was “without authority” to enjoin defendant “as a precautionary measure” without any factual findings or pointing to evidence in the record to support such restrictions). As this Court has recognized, these principles apply with equal force in this litigation. *See* Tr. 4:20-23.

The first proposed audit encompasses “*any* new disclosure,” including “*any* new grants of access” of PII that exists in “in *any* OPM systems of records,”—*i.e.*, nearly every data system at OPM—to *anyone* (both OPM employees and non-OPM employees) from March 6 to the present. This proposed audit is not tied to Plaintiffs' allegations and the Court's factual findings or conclusions of law.⁸ As noted above, the Court has defined the “final agency action” in this case as “[t]he decision to give access to DOGE agents,” specifically “administrative access to multiple OPM systems for DOGE agents.” ECF No. 121 at 88. Enlarging the ambit of this case to any disclosure or any grant of access (regular user access or administrative access) to any OPM data systems is not supported by the Court's findings of fact or conclusions of law—and it would not preserve the status quo.

Moreover, both the first and second proposed audits are unsupported by factual findings or evidence in the record. As the Court notes, it has “no insight into what happened after March 6, and obviously the plaintiffs don't.” Tr. 8:16-17; *see also* Tr. 9:16-18. These suggested audits are thus untethered to any evidence of even a likely Privacy Act violation. The only explanation for such recurring audits is to allow the Court to oversee, writ large, and on an ongoing basis, OPM's day-to-day compliance with its obligations under the Privacy Act. Such injunctive relief is thus impermissible.

The third proposed audit similarly has no basis in the Court's findings of fact and conclusions of law. While the Court found that extracted data—specifically, “names and Government email addresses”—from OPM data systems were “records [that] were disclosed to

⁸ To the extent the second proposed audit requires the agency to provide additional information concerning grants of access to “DOGE Agents” (as newly defined), and to now include information concerning “regular user access” as well, it is similarly without any evidentiary basis. Furthermore, to the extent the second proposed audit requires the agency to supplement the administrative record by responding to a Court-ordered interrogatory, it represents impermissible discovery in this APA action, and usurps the agency's role in compiling the administrative record.

and reviewed by DOGE agents,” ECF No. 121 at 74 n.36,⁹ crucially, this Court never found that such “disclosure” amounted to a likely violation of the Privacy Act. *See id.* That is presumably because such information was disclosed to OPM employees who had a need for the record in performance of their duties, *see* Defs’ Mem. of Law (ECF No. 95), at 14-15 & n.11. There is simply no evidence in the record that “copies of records or copies of information extracted from records,” ECF No. 129-1 at 5, were ever made *in violation of* the Privacy Act. Moreover, there is no evidence that either career OPM staff used their access to agency data systems to improperly disclose PII to “DOGE agents,” or that “DOGE agents” somehow requested or obtained such records under false pretenses, in violation of the Privacy Act—both of which would be *criminal offenses*. *See* 5 U.S.C. § 552a(i)(1), (2). Accordingly, the third proposed forensic audit is an injunction that is foreclosed under Second Circuit precedent. *See Faiveley Transp.*, 559 F.3d at 120.

While Defendants maintain that a preliminary injunction is unwarranted, only Defendants’ proposal is narrowly tailored to the specific violations the Court found—*i.e.*, granting of administrative access to OPM’s “DOGE agents,” ECF No. 121 at 81, 88—and the irreparable harm it cited—“increased risk of cybersecurity breaches,” *id.* at 95. And Defendants’ proposal would do the least amount of harm to OPM’s important operations.

Disruption to OPM’s Operations and Inadequacy of the Court’s Proposed Security

To the extent the Court were to issue the draft preliminary injunction order requiring OPM to conduct these three forensic audits, it would severely disrupt OPM’s operations. As such, the proposed security amount of \$1,000 is exceedingly inadequate to pay the cost and damages OPM will sustain if it is later found to have been wrongfully enjoined. *See* Fed. R. Civ. P. 65(c). As Defendants previously noted at the June 13 conference, Tr. 12:9-14:7, such an injunction would require OPM to devote dozens of OPM employees within OPM’s Office of the Chief Information Officer, OPM’s Chief Information Security Officer, OPM’s human resources department, and OPM’s Personnel Security Division to this effort, all on the shortest of timeframes.

For example, to conduct only the first of the three forensic audits proposed by the Court (and now Plaintiffs), OPM would need to request information on any new grant of access to users—administrative or regular users (which would include even career OPM employees who have been at OPM for decades but were recently granted new user access to any of these systems)—from each of the database administrators who oversee OPM’s approximately 50 separate data systems that house PII. Next, OPM would need to ask OPM’s database administrators to determine whether any “new disclosure” of records occurred from each of OPM’s 50 data systems by conducting a forensic audit to determine if any data was exported from each system,

⁹ The Court’s Opinion notes that “[i]ndividuals working on the DOGE agenda in connection with the creation of GWES were given at least names and Government email addresses that were extracted from OPM systems by career OPM employees,” *id.*, and that “Hogan also testified that career OPM employees may also have disclosed OPM records to individuals working on the DOGE agenda in other contexts, including in connection with a retirement services modernization project,” *id.* However, the Court never found that any of these disclosures were *impermissible* under the Privacy Act.

by whom, and whether such data was further provided to any other employee within OPM or otherwise, which will likely involve in-person interviews with each individual employee at issue. Once the universe of relevant employees is defined, OPM would then need to determine whether *each* of these employees completed all training—including the type of training they received and when, and whether they were appropriately vetted (in some cases dozens of years ago).

OPM *conservatively* estimates that such initial audit would require at least 1000 employee hours to complete. Utilizing an hourly rate of \$33.50 per hour for a GS-9 employee (the lowest graded position that would be able to perform this type of forensic information technology audit),¹⁰ the total cost of this single forensic audit would amount to \$33,500.00. That figure does not account for the fact that this audit would be required to be completed on a monthly basis, nor that it would necessarily divert employees from important work modernizing OPM's IT systems and ensuring OPM's day-to-day operations continue in an appropriate manner. The costs of the second and third forensic audits proposed by the Court would likely entail even greater costs, as they would require substantial resources to plan, conduct, and complete, so that accurate certifications could be provided to the Court, under pain of contempt. As a result, OPM conservatively estimates that these three proposed forensic audits would cost, *at least*, \$100,000.00 to complete. Accordingly, to the extent the Court issues its draft preliminary injunction order, the amount of security required by the Court should be increased to at least this amount.

We thank the Court for its consideration of this submission.

Respectfully submitted,

JAY CLAYTON
United States Attorney for the
Southern District of New York

By: /s/ David Farber
JEFFREY OESTERICH
DAVID E. FARBER
Assistant United States Attorneys
86 Chambers Street, Third Floor
New York, New York 10007
Tel.: (212) 637-2695/2772

Encl.

cc: Plaintiffs' counsel (by ECF)

¹⁰ See OPM, *GS-2210: Information Technology Management Series*, available at <https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/0300/gs-2210-information-technology-management-series/>; OPM, *Hourly Salary Table, Area of Washington-Baltimore-Arlington* (2025), available at https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2025/DCB_h.pdf.